REMARKS

The Examiner has rejected Claims 1-16 under 35 U.S.C. 101 as being directed toward non-statutory subject matter. Applicant has clarified Claim 1 to include a computer program product "embodied on a tangible computer readable medium" in order to avoid such rejection.

The Examiner has rejected Claims 1, 3-6, 8-16, 17, 19-22, 24-32, 33, 35-38, and 40-47 under 35 U.S.C. 103(a) as being unpatentable over Nambu (U.S. Patent Publication No. 2002/0124182), in view of Hershberg et al. (U.S. Patent Publication No. 2003/0022657). Applicant respectfully disagrees with such rejection.

With respect to the independent claims, the Examiner has relied on the following excerpts from the Nambu reference to make a prior art showing of applicant's claimed "identifying one or more classes of malware threat against which said mobile computing device is to be protected" (see this or similar, but not necessarily identical language in the independent claims).

> "In accordance with the circumstances under which viruses are generated, the maintenance server 41 registers and manages the information of new types of viruses. The information of the new virus includes, for example, virus name, danger level, discovery data, vaccine manufacture date (vaccine manufacture schedule), and the corresponding pattern file name (pattern number). The maintenance server 41 receives and stores updated vaccine software (including scan engines) and pattern data files that are provided by each company.
>
> The support computers 42a, 42b of the vaccine software makers may upload vaccine software and pattern files to the maintenance server 41.
>
> The maintenance server 41 is connected to various user terminals (in FIG. 5, four terminals) 45a, 45b, 45c, 45d by a public line 46, which includes the internet. The first terminal 45a is, for example, a cellular phone, and the second terminal 45b is, for example, a portable terminal such as a personal digital assistant (PDA) The third terminal 45c is, for example, a computer system of a personal computer, and the fourth terminal 45d is for example, a game device of a home communication terminal (set-top box) provided with a communication function." (paragraphs [0072]-[0074] - emphasis added)

More specifically, the Examiner asserts that "it is known within existing malware definition data to include information that classifies the malware items using classes." However, applicant respectfully disagrees and notes that the above excerpts relied on by the Examiner merely teach that a "maintenance server... registers and manages the information of new types of viruses" and that "[t]he maintenance server... receives and stores updated vaccine software (including scan engines) and pattern data files" (paragraph [0072] – emphasis added). Further, the excerpts teach that "support computers... of the vaccine software makers may upload vaccine software and pattern files to the maintenance server" and that [t]he maintenance server... is connected to various user terminals" (paragraphs [0073]-[0074] – emphasis added).

However, registering and managing new virus types, receiving and storing updated vaccine software and pattern data files, and uploading vaccine software to a server which is connected to user terminals, as in Nambu, does not teach "identifying one or more classes of malware threat against which said mobile computing device is to be protected" (emphasis added), as claimed by applicant. Additionally, it appears that the Examiner has relied on an inherency argument regarding the above emphasized claim limitations. In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested (See MPEP 2112).

Additionally, with respect to the independent claims, the Examiner has relied on the following excerpts from the Nambu reference to make a prior art showing of applicant's claimed "generating from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected" (see this or similar, but not necessarily identical language in the independent claims).

"The maintenance server 41 stores information related to the user terminals 45a-45d and, based on the user-related information, provides the terminals 45a-45d with updated vaccine software and pattern files." (paragraph [0075] - emphasis added)

"The maintenance server 41 includes a new anti-virus processing program 51, a resource distribution program 52, and information files 53, 54. The maintenance server 41 stores vaccine software and pattern files 55, 56 that are received from the vaccine software makers.

The new anti-virus processing program 51 includes a new virus information processing program 51a and a user information processing program 51b. The first information file 53 functions as a new virus countering information memory and stores vaccine software information (name of virus for which a vaccine has been produced, name of pattern file of virus for which a vaccine has been produced, name of virus for which a vaccine has not yet been produced, and danger level). The second information file 54 functions as a user information memory. The file 54 stores the present condition of the user terminal (information indicating the presently used vaccine software and whether to constantly update the vaccine software (including that of other manufacturers))." (paragraphs [0077]-[0078] - emphasis added)

Applicant respectfully points out that the above excerpts relied on by the Examiner merely teach that a "maintenance server… stores information related to the user terminals" and "provides the terminals… with updated vaccine software and pattern files" (emphasis added). Additionally, the excerpts teach that "[t]he maintenance server 41 stores vaccine software and pattern files" (emphasis added). Further, the excerpts teach that "[t]he first information file… functions as a new virus countering information memory and stores vaccine software information" and that "[t]he second information file… stores the present condition of the user terminal" (emphasis added).

However, merely storing vaccine software and pattern files and information, in addition to storing the present condition of a user terminal, as in Nambu, fails to disclose "generating from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected" (emphasis added), as claimed by applicant. Clearly, merely storing pattern

files and information, as in Nambu, simply fails to even suggest "classes of malware threat against which said mobile computing device is to be protected" (emphasis added), in the manner as claimed by applicant.

Further, with respect to the independent claims, the Examiner has relied on paragraphs [0074], [0075], and [0077] from the Nambu reference (reproduced above) to make a prior art showing of applicant's claimed technique "wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully notes that the above reference excerpts relied on by the Examiner merely disclose that "[t]he maintenance server... is connected to various user terminals" (paragraph [0074] – emphasis added), that "[t]he maintenance server 41 stores information related to the user terminals" (paragraph [0075] – emphasis added), and that "[t]he maintenance server... stores vaccine software and pattern files... that are received from the vaccine software makers" (paragraph [0077] – emphasis added).

However, merely storing information related to user terminals, in addition to storing vaccine software and pattern files, as in Nambu, fails to teach a technique "wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable" (emphasis added), as claimed by applicant. Clearly, storing information relating to user terminals and providing updated vaccine software and pattern files, as in Nambu, simply fails to suggest "transfer[ing] computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable" (emphasis added), as claimed by applicant.

Further still, with respect to the independent claims, the Examiner has relied on paragraph [0078] (reproduced above), in addition to the following excerpts, from the Nambu reference to make a prior art showing of applicant's claimed technique "wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies" (see this or similar, but not necessarily identical language in the independent claims).

> "The new anti-virus processing program 51 acquires the vaccine software-related information from the second information file 54 via the user information processing program 51b. The processing program 51 acquires the new virus countering information that corresponds to the vaccine software-related information from the first information file 53 via the new virus information processing program 51a." (paragraph [0081] - emphasis added)

> "The maintenance server 41 determines whether the vaccine software and pattern data files presently used by the user terminals 45a-45d are capable of countering a new virus from the countering information file 53 and the user-related information file 54. Based on the determination, the resource distribution program 52 distributes to the user terminals 45a-45d, vaccine software and pattern files (including that of other makers) that have been updated to counter the new virus." (paragraph [0108] - emphasis added)

Applicant respectfully points out that the above excerpts relied on by the Examiner merely disclose that "[t]he first information file... functions as a new virus countering information memory and stores vaccine software information" and that "[t]he second information file... stores the present condition of the user terminal" (paragraph [0078] - emphasis added). Additionally, the above excerpts teach that the "new anti-virus processing program... acquires the vaccine software-related information" as well as "new virus countering information." Further, the excerpts teach that "[t]he maintenance server... determines whether the vaccine software and pattern data files presently used... are capable of countering a new virus" and that "[b]ased on the determination, the resource distribution program... distributes to the user terminals... vaccine software and pattern files... that have been updated to counter the new virus" (emphasis added).

However, merely acquiring vaccine and virus countering information, determining whether a vaccine is capable of countering a new virus, and distributing vaccine software based on the determination, as in Nambu, fails to suggest a technique "wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies" (emphasis added), as claimed by applicant. Clearly, distributing vaccine software based on the determination if the vaccine is capable of countering a new virus, as in Nambu, simply fails to even suggest that "one or more classes of malware threat... are chosen according to classes of malware threat known to pose a problem to said mobile computing device" (emphasis added), in the manner as claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 4 et al., the Examiner has relied on paragraphs [0074], [0075], and [0077] from the Nambu reference (reproduced above) to make a prior art showing of applicant's claimed technique "wherein, when said mobile

computing device is connected to said fixed location computing device, different versions of user generated computer files respectively stored by said mobile computing device and said fixed location computing device are synchronized."

Applicant respectfully notes that the above excerpts relied on by the Examiner merely teach that a "maintenance server... is connected to various user terminals" and that "[t]he maintenance server... stores information related to the user terminals... and, based on the user-related information, provides the terminals... with updated vaccine software" (paragraph [0074]). Also, the above excerpts teach that "[t]he maintenance server... stores vaccine software and pattern files... that are received from the vaccine software makers" (paragraph [0077] – emphasis added).

However, merely teaching that a maintenance server is connected to user terminals, stores vaccine files received from vaccine software makers, and provides the terminals with updated vaccine software, as in Nambu, fails to suggest a technique "wherein, when said mobile computing device is connected to said fixed location computing device, different versions of user generated computer files respectively stored by said mobile computing device and said fixed location computing device are synchronized" (emphasis added), as claimed by applicant. Clearly, vaccine files received from vaccine software markers, as in Nambu, simply fails to even suggest that "different versions of user generated computer files respectively stored by said mobile computing device and said fixed location computing device are synchronized" (emphasis added), as claimed by applicant.

Additionally, with respect to Claim 8 et al., the Examiner has relied on the following excerpt from the Nambu reference to make a prior art showing of applicant's claimed technique "wherein user controlled policy data is used in combination with said threat data to control against which classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data."

> "When the vaccine software used by the presently connected user terminal does not correspond to the new virus and the user wishes

> to constantly update the vaccine software (including that of other manufacturers), the new anti-virus processing program 51 provides the resource distribution program 52 with information for sending vaccine software corresponding to the new virus to the user terminal." (paragraph [0082])

Applicant respectfully notes that the above excerpt relied on by the Examiner merely discloses that "[w]hen the vaccine software used by the presently connected user terminal does not correspond to the new virus and the user wishes to constantly update the vaccine software" the "anti-virus processing program... provides the resource distribution program... with information for sending vaccine software corresponding to the new virus to the user terminal" (emphasis added).

However, the mere disclosure of the user wishing to constantly update the vaccine software, in addition to the resource distribution program sending vaccine software to the user terminal, as in Nambu, does not teach a technique "wherein user controlled policy data is used in combination with said threat data to control against which classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data" (emphasis added), as claimed by applicant. Clearly, sending vaccine software to the user terminal when the vaccine software used by the user terminal does not correspond to the new virus, as in Nambu, simply fails to even suggest "control[ling] against which classes of malware threat said mobile computing device is protected" (emphasis added), in the manner as claimed by applicant.

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 49-50 below, which are added for full consideration:

"wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to said classes of malware threat known to pose a problem to an operating system of said mobile computing device" (see Claim 49); and

"wherein at least a portion of said mobile computing device malware definition data poses a problem only to said mobile computing device and not to said fixed location computing device" (see Claim 50).

Again, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P482).

Respectfully submitted,
Zilka-Kotab, PC.

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100